****

 **St Ignatius Primary School**

**E-Safety Policy**

|  |  |
| --- | --- |
| Policy Originator | St Ignatius Primary School  |
| Governor Responsible | Lourdes Keever |
| Status | Statutory  |
| Last reviewed  | March 2019 |
| Ratified on  |  |
| To be next reviewed  | March 2020 |
| Signed  |  |

**Introduction**

At St Ignatius Catholic Primary School we understand the responsibility we have to educate our pupils on e-safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy forms an important part of St Ignatius School’s Safeguarding policy and should be read in conjunction with our Anti-bullying, Behaviour policy and Photography and Video policy.

 **Background/Rationale**

New technologies have become integral to the lives of children and young people in today’s society, both within schools and their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school e-Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child’s education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students/pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student/pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they face include:

* Access to illegal, harmful or inappropriate images or other content;
* Un-authorized access to/loss of/ sharing of personal information;
* The risk of being subject to grooming by those with whom they make contact on the internet;
* The sharing/distribution of personal images with/without an individual’s consent or knowledge;
* Inappropriate communication/contact with others, including strangers;
* Cyber-bullying;
* Sexting;
* Access to unsuitable video/internet games;
* An inability to evaluate the quality, accuracy and relevance of information on the internet;
* Plagiarism and copyright infringement;
* Illegal downloading of music or video files;
* The potential for excessive use which may impact on the social and emotional development and learning of the young person.

 **Aims**

Our school aims to:

* Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
* Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
* Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

#  Legislation and guidance

 This policy is based on the Department for Education’s statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on [preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation). It also refers to the Department’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the [National Curriculum computing programmes of study](https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study).

**Roles and Responsibilities**

**Governors**

Governors are responsible for the approval of the e-safety Policy and for reviewing the effectiveness of the policy. Any e-safety incidents of issues will be discussed during the curriculum meetings or with the school safeguarding governor (Lourdes Keever).

**Headteacher and Senior Leadership Team**

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

**The designated safeguarding leads**

Details of the school’s designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

* Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
* Working with the headteacher and other staff, as necessary, to address any online safety issues or incidents
* Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
* Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behavior policy
* Updating and delivering staff training on online safety
* Liasing with other agencies and/or external services if necessary
* Providing regular reports on online safety in school to the headteacher and/or governing board

**The ICT Manager**

The ICT manager is responsible for:

* Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
* Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
* Conducting a full security check and monitoring the school’s ICT systems on a weekly basis
* Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
* Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behavior policy

**All staff and volunteers**

All staff, including contractors and agency staff, and volunteers are responsible for:

* Maintaining an understanding of this policy
* Implementing this policy consistently
* Agreeing and adhering to the terms on acceptable use of the school’s ICT systems and the internet, and ensuring that pupils follow the school’s terms on acceptable use
* Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with the policy
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behavior policy

**Parents**

Parents are expected to:

* Notify a member of staff or the headteacher of any concerns or queries regarding this policy
* Ensure their child has read, understood and agreed to the terms on acceptable use of the school’s ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organizations and websites:

What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>

Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>

Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

**Visitors and members of the community**

Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix)

**Teachers**

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow e-safety procedures.

All staff should be familiar with the school’s policy including:

* safe use of email
* safe use of the internet
* safe use of the school network, equipment and data
* safe use of digital images and digital technologies, such as mobile phones and digital cameras
* publication of pupil information/photographs on the school website
* procedures in the event of misuse of technology by any member of the school community
* their role in providing e-safety education for pupils
* Staff are reminded/updated about e-safety regularly and new staff receive information on the school’s acceptable use policy as part of their induction.

 Managing the school e-safety messages

* We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
* The e-safety policy will be shared with new staff, including the acceptable use policy as part of their induction.

#  Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

 Pupils in **Key Stage 2** will be taught to:

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

 The school will use assemblies to raise pupils’ awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.The children will also take part in Internet Safety Week and Anti-Bullying week where Internet Safety and Cyber Bullying are a focus.

 **Educating parents about online safety**

The school will raise parents’ awareness of internet safety in letters or other communications home, and in information via our website. As a school we will also offer workshops where parents can come and discuss concerns re internet safety, Information on parental controls will be shared with parents and any issues that arise in the media where parents needs to be informed or updated will also be part of our communication with our parents. As a school we regularly share information with parents about the terms of agreement (age of consent) of social media apps on mobile phones. As a school we take cyber bullying on social media very seriously (see social media policy). This policy will also be shared with parents.

Online safety will also be covered during parents’ evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

# Cyber-bullying

# Definition:

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

**Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training .

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

**6.3 Examining electronic devices**

**At St Ignatius Mobile phones are only allowed in school if parents have written to the headteacher. The reason phones are allowed (smartphones not included) are if parents wish their child to have a phone on their journey to and from school and for safety reasons.**

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils’ electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a ‘good reason’ to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or

Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

Report it to the police

Any searching of pupils will be carried out in line with the DfE’s latest guidance on [screening, searching and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation).

Any complaints about searching for or deleting inappropriate images or files on pupils’ electronic devices will be dealt with through the school complaints procedure.

**Acceptable use of the internet in school**

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet (see appendix). Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in the appendix.

# Pupils using mobile devices in school

**See above school’s stance on mobile phones**

Pupils may bring mobile devices into school ( if written requests by parents are accepted), but are not permitted to use them during:

Lessons

Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

**Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use, as set out in appendix.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

 **How the school will respond to issues of misuse**

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school’s ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

# Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL [ and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

# Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in theappendix.

This policy will be reviewed yearly by the DSL. At every review, the policy will be shared with the governing board.

# Links with other policies

 This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure